Implementasi Cipher Hill pada kode ASCII dengan Memanfaatkan Digit Desimal Bilangan Euler

Oleh :
Kuswari Hernawati
Jurusan Pendidikan Matematika
FMIPA Universitas Negeri Yogyakarta
Alamat: Jl. Colombo Karangmalang Yogyakarta 55281

Abstrak

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dalam suatu sistem informasi, dalam hal ini sangat terkait dengan betapa pentingnya informasi tersebut dikirim dan diterima oleh orang yang berkepentingan. Informasi tidak akan berguna lagi apabila di tengah jalan informasi tersebut disadap atau dibajak orang yang tidak berhak. Cara yang ditempuh adalah dengan kriptografi yang menggunakan transformasi data sehingga data yang dikirimkan tidak mudah dimengerti oleh pihak ketiga, salah satu cara transformasi data adalah dengan cipher hill.

Keunikan digit desimal dari bilangan Euler (biasa disebut bilangan e) dapat digunakan sebagai acuan penerapkan algoritma yang ada di kajian kriptografi. Hal ini dengan pertimbangan bahwa pembangkitan bilangan/kode acuan dapat diperoleh dari formulasi perhitungan digit desimal bilangan Euler yang sudah mapan dan diakui dunia.

Selain itu, deretan digit dari nilai desimal bilangan e untuk implementasi enkripsi-dekripsi dengan cipher hills yaitu dengan cara pengelompokan digit berdasar kunci yang digunakan sangat kecil kemungkinannya menghasilkan nilai rujukan yang sama.

Kata kunci : Euler, transformasi data, kriptografi, hill

Latar Belakang

Perkembangan teknologi telekomunikasi dan penyimpanan data dengan menggunakan komputer memungkinkan pengiriman data jarak jauh yang relatif cepat dan murah. Di sisi lain pengiriman data jarak jauh memungkinkan pihak lain dapat menyadap dan mengubah data yang dikirimkan, sehingga perlu adanya keamanan data di dalamnya. Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dalam suatu sistem informasi, dalam hal ini sangat terkait dengan betapa pentingnya informasi tersebut dikirim dan diterima oleh orang yang berkepentingan. Informasi tidak akan berguna lagi apabila di tengah jalan informasi tersebut disadap atau dibajak orang yang tidak berhak. Cara yang ditempuh adalah dengan kriptografi yang menggunakan transformasi data sehingga data yang dikirimkan tidak mudah dimengerti oleh pihak ketiga, salah satu cara transformasi data adalah dengan cipher hill.

Pada makalah ini akan dibahas bagaimana digit desimal dari bilangan Euler (biasa disebut bilangan e) digunakan sebagai acuan penerapan algoritma cipher hill pada kode ASCII. Hal ini dengan pertimbangan bahwa pembangkitan bilangan/kode acuan dapat

Dipresentasikan dalam Seminar Nasional MIPA 2006 dengan tema **"Penelitian, Pendidikan, dan Penerapan MIPA serta Peranannya dalam Peningkatan Keprofesionalan Pendidik dan Tenaga Kependidikan"** yang diselenggarakan oleh Fakultas MIPA UNY, Yogyakarta pada tanggal 1 Agustus 2006

diperoleh dari formulasi perhitungan digit desimal bilangan Euler yang sudah mapan dan diakui dunia.

Bilangan Euler

Bilangan e yang kemudian disebut sebagai bilangan euler merupakan bilangan yang diperoleh dari pendekatan nilai $(1+1/n)^n$ untuk n menuju tak hingga, yang ditemukan pada tahun 1683 oleh Jacob Bernoulli.

$$e = \lim_{n\to\infty}(1+\tfrac{1}{n})^n$$

Pada tahun 1748 , Euler memberikan ide mengenai bilangan e yaitu

$e = 1+ 1/1! + 1/2! + 1/3! + 1/4! + ...$ dan bahwa $e = \lim_{n\to\infty}(1+\tfrac{1}{n})^n$. Dari formulasi tersebut, Euler memberikan pendekatan untuk bilangan e 18 digit dibelakang koma, yaitu: e= 2,718281828459045235

Pada tahun 1884 Boorman menghitung e sampai dengan 346 digit dibelakang koma dan telah dihitung sampai dengan 869.894.101 digit dibelakang koma oleh Sebastian Wedeniwski. (O'Connor, 2001)

e =

2.71828182845904523536028747135266249775724709369995957496696762772407663035354759457138217852516642742746639193200305992181741359662904357290033429526059563073813232862794349076323382988075319525101901157383418793070215408914993488416750924476146066808226480016847741185374234544243710753907774499206955170276183860626133138458300075204493382656029760673711320070932870912744374704723069697720931014169283681902551510865746377211125238978442505695369677078544996996794686445490598793163688923009879312773617821542499922957635148220826989519366803318252886939849646510582093923982948879332036250944311730123819706841614039701983767932068328237646480429531180232878250981945581530175671736133206981125099618188159304169035159888851934580727386673858942287922849989208680582574927961048419844436346324496848756023362482704197862320900216099023530436994184914631409343173814364054625315209618369088870701676839642437814059271456354906130310720851038375051011574770417189861068739696552126715468895703503540212340784981933432106817012100562788023519303322474501585390473041995777709350366041699732972508868769664035557071622684471625607988265178713419512466520103059212366771943252786753985589448969709640975459185695638023637016211204774272283648961342251644507818244235294863637214174023889344124796357437026375529444833799801612549227850925778256209262264832627793338656648162772516401910590049164499828931505660472580277863186415519565324425869829469593080191529872117255634754639644791014590409058629849679128740687050489585867174798546677575732056812884592054133405392200011378630094556068816674001698420558040336379537645203040243225661352783695117788386387443966253224985065499

5886234281899707733276171783928034946501434558897071942586398772754710
9629537415211151368350627526023264847287039207643100595841166120545297
0302364725492966693811513732275364509888903136020572481765851180630364
4281231496550704751025446501172721155519486685080036853228183152196003
7356252794495158284188294787610852639813955990067376482922443752871846
2457803619298197139914756448826260390338144182326251509748279877799643
7308997038886778227138360577297882412561190717663946507063304527954661
8550966661856647097113444740160704626215680717481877844371436988218559
6709591025968620023537185887485696522000503117343920732113908032936344
7972735……

Kode ASCII

Kode ASCII (Standard Code for Information Interchange) merupakan representasi numerik dari suatu karakter seperti ‘a’ atau ‘@’ atau karakter yang tidak tercetak, misalnya ‘Σ’. Tabel dibawah ini menunjukkan karakter ASCII termasuk 32 karakter yang tidak tercetak.

Desimal	Karakter	Desimal	Karakter	Desimal	Karakter	Desimal	Karakter
0	NUL	32	Space	64	@	96	`
1	SOH	33	!	65	A	97	a
2	STX	34	“	66	B	98	b
3	ETX	35	#	67	C	99	c
4	EOT	36	$	68	D	100	d
5	ENQ	37	%	69	E	101	e
6	ACK	38	&	70	F	102	f
7	BEL	39	‘	71	G	103	g
8	BS	40	(	72	H	104	h
9	TAB	41	)	73	I	105	i
10	LF	42	*	74	J	106	j
11	VT	43	+	75	K	107	k
12	FF	44	,	76	L	108	l
13	CR	45	-	77	M	109	m
14	SO	46	.	78	N	110	n
15	SI	47	/	79	O	111	o
16	DLE	48	0	80	P	112	p
17	DC1	49	1	81	Q	113	q

18	DC2	50	2	82	R	114	r
19	DC3	51	3	83	S	115	s
20	DC4	52	4	84	T	116	t
21	NAK	53	5	85	U	117	u
22	SYN	54	6	86	V	118	v
23	ETB	55	7	87	W	119	w
24	CAN	56	8	88	X	120	x
25	EM	57	9	89	Y	121	y
26	SUB	58	:	90	Z	122	z
27	ESC	59	;	91	[	123	{
28	FS	60	<	92	\	124	|
29	GS	61	=	93	]	125	}
30	RS	62	>	94	^	126	~
31	US	63	?	95	_	127	DEL

32 Karakter tidak tercetak

128	Ç	144	É	161	í	177	▒	193	┴	209	╤	225	ß	241	±
129	ü	145	æ	162	ó	178	▓	194	┬	210	╥	226	Γ	242	≥
130	é	146	Æ	163	ú	179	|	195	├	211	╙	227	π	243	≤
131	â	147	ô	164	ñ	180	┤	196	─	212	╘	228	Σ	244	⌠
132	ä	148	ö	165	Ñ	181	╡	197	┼	213	╒	229	σ	245	⌡
133	à	149	ò	166	ª	182	╢	198	╞	214	╓	230	µ	246	÷
134	å	150	û	167	º	183	╖	199	╟	215	╫	231	τ	247	≈
135	ç	151	ù	168	¿	184	╕	200	╚	216	╪	232	Φ	248	°
136	ê	152	_	169	_	185	╣	201	╔	217	┘	233	Θ	249	·
137	ë	153	Ö	170	¬	186	║	202	╩	218	┌	234	Ω	250	·
138	è	154	Ü	171	½	187	╗	203	╦	219	▒	235	δ	251	√
139	ï	156	£	172	¼	188	╝	204	╠	220	▄	236	∞	252	_
140	î	157	¥	173	¡	189	╜	205	═	221	▌	237	ϕ	253	²
141	ì	158	_	174	«	190	╛	206	╬	222	▐	238	ε	254	■
142	Ä	159	ƒ	175	»	191	┐	207	╧	223	▀	239	∩	255	
143	Å	160	á	176	▒	192	└	208	╨	224	α	240	≡		

Kriptografi

Kriptografi adalah ilmu yang mempelajari bagaimana membuat suatu pesan yang dikirim pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi dapat memenuhi kebutuhan umum suatu transaksi. Kebutuhan untuk kerahasiaan

(*confidentiality*) dengan cara melakukan enkripsi (penyandian). Keutuhan (*integrity*) atas data-data pembayaran dilakukan dengan fungsi hash satu arah.

Jaminan atas identitas dan keabsahan (*authenticity*) pihak-pihak yang melakukan transaksi dilakukan dengan menggunakan password atau sertifikat digital. Sedangkan keotentikan data transaksi dapat dilakukan dengan tanda tangan digital. Transaksi dapat dijadikan barang bukti yang tidak bisa disangkal (*non-repudiation*) dengan memanfaatkan tanda tangan digital dan sertifikat digital.

Pembakuan penulisan pada kriptografi dapat ditulis dalam bahasa matematika. Fungsi-fungsi yang mendasar dalam kriptografi adalah enkripsi dan dekripsi. Enkripsi adalah proses mengubah suatu pesan asli (*plaintext*) menjadi suatu pesan dalam bahasa sandi (*ciphertext*).

C = E (M)

dimana

M = pesan asli

E = proses enkripsi

C = pesan dalam bahasa sandi (untuk ringkasnya disebut sandi)

Sedangkan dekripsi adalah proses mengubah pesan dalam suatu bahasa sandi menjadi pesan asli kembali.

M = D (C)

D = proses dekripsi

Umumnya, selain menggunakan fungsi tertentu dalam melakukan enkripsi dan dekripsi, seringkali fungsi itu diberi parameter tambahan yang disebut dengan istilah kunci. Terdapat tiga kategori enkripsi, yaitu: (1) kunci enkripsi rahasia, dalam hal ini terdapat sebuah kunci yang digunakan untuk mengenkripsi dan juga sekaligus mendekripsi informasi, (2) kunci enkripsi publik, menggunakan dua kunci satu untuk proses enkripsi dan satu untuk proses dekripsi, dan (3) fungsi one-way, atau fungsi satu arah adalah suatu fungsi di mana informasi dienkripsi untuk menciptakan “signature” dari informasi asli yang bisa digunakan untuk keperluan autentifikasi.

(Wibowo, 1997)

Model-model enkripsi

1. Enkripsi dengan kunci Pribadi

Enkripsi ini dapat dilakukan jika si pengirim dan si penerima telah sepakat menggunakan kunci dan metode enkripsi tertentu. Metode enkripsi atau kunci yang digunakan harus dijaga agar tidak ada pihak luar yang mengetahuinya. Kesepakatan cara enkripsi atau kunci enkripsi ini bisa dicapai lewat jalur komunikasi lain yang lebih aman, misalnya dengan pertemuan langsung. Cara enkripsi dengan kesepakatan atau kunci enkripsi ini dikenal dengan istilah enkripsi dengan kunci pribadi, karena kunci hanya boleh diketahui oleh dua pribadi yang berkomunikasi tersebut.

Cara enkripsi dengan kunci pribadi umumnya digunakan untuk kalangan bisnis maupun pemerintahan. Beberapa metode yang termasuk dalam enkripsi dengan kunci pribadi antara lain: *substitution cipher* yang meliputi *simple substitution* (Caesar cipher/*mono alphabetical cipher*), *homophonic substitution, poly alphabetic subtitution, polygraphic substitution.*

Dari beberapa metode di atas, di dalam pembahasan makalah ini hanya digunakan *polygraphic substitution cipher.* Dalam *polygraphic substitution cipher* plaintext disubstitusikan dalam kelompok-kelompok yang lebih besar, yang akan menggantikan substitusi teks per huruf/abjad. Hill cipher merupakan *polygraphic substitution* yang dapat mengkombinasikan lebih banyak huruf secara berturut-turut menggunakan aljabar linier. Hill cipher dibuat tahun 1929 oleh Lester S. Hill. Tiap-tiap huruf diperlakukan sebagai sebuah digit dalam basis 26, misalnya A = 0, B = 1, C = 3 dst. Sebuah blok dari n huruf dinyatakan sebagai vektor dimensi n, dan dikalikan dengan matriks nxn, modulo 26. Komponen matriks merupakan kunci, dipilih random dengan syarat merupakan matriks invertibel untuk memastikan bahwa dekripsi mungkin dilakukan.

Misalnya diambil sebuah kunci matriks berukuran 3x3

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$$

Jika akan dienkripsi sebuah pesan ‘CAT’, dimana C = 2, A=0 dan T =19, maka pesan diubah dalam bentuk matriks berukuran 3x1 dan akan dienkripsi menjadi

$$\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 31 \\ 216 \\ 325 \end{pmatrix} \equiv \begin{pmatrix} 5 \\ 8 \\ 13 \end{pmatrix} \mod 26$$

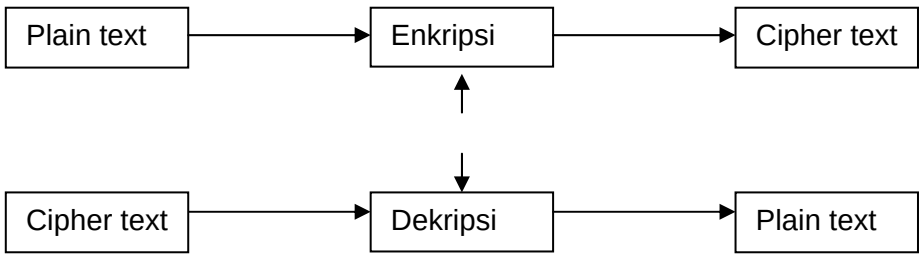
Matriks $\begin{pmatrix} 5 \\ 8 \\ 13 \end{pmatrix}$, dikonversikan dalam bentuk huruf/abjad menjadi 'FIN', sehingga pesan 'CAT' setelah dienkripsi menjadi pesan 'FIN'.

Untuk mendekripsi pesan kembali, maka dicari invers modulo 26 dari matriks kunci $\begin{pmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{pmatrix}$, sehingga diperoleh matriks inversnya adalah $\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix}$.

Pesan yang diterima 'FIN' dalam bentuk matriks $\begin{pmatrix} 5 \\ 8 \\ 13 \end{pmatrix}$, didekripsi dengan dikalikan matriks invers modulo 26 dari matriks kunci

$\begin{pmatrix} 8 & 5 & 10 \\ 21 & 8 & 21 \\ 21 & 12 & 8 \end{pmatrix} x \begin{pmatrix} 5 \\ 8 \\ 13 \end{pmatrix} = \begin{pmatrix} 210 \\ 442 \\ 305 \end{pmatrix} = \begin{pmatrix} 2 \\ 0 \\ 19 \end{pmatrix} \text{mod } 26$, yang akan mengembalikan ke pesan semula yaitu 'CAT'

Proses enkripsi-dekripsi dengan menggunakan algoritma dari enkripsi kunci pribadi dapat digambarkan sebagai berikut:



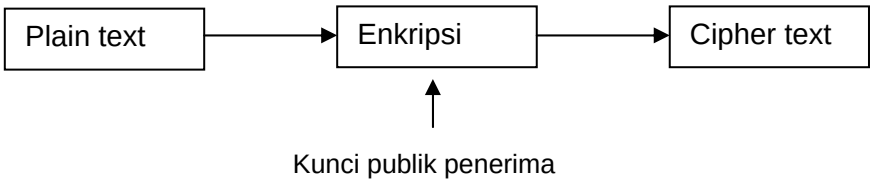
Gambar 1. Algoritma enkripsi dengan kunci pribadi

Dalam algoritma kunci pribadi, kunci digunakan untuk enkripsi data dan tidak diberikan kuasa kepada publik tetapi hanya pada orang tertentu yang tahu dan dapat membaca data yang dienkripsi. Karakteristik dari algoritma kriptografi kunci pribadi adalah bahwa kunci enkripsi sama dengan kunci dekripsi. (Kristanto, 2003)

2. Enkripsi dengan kunci Publik

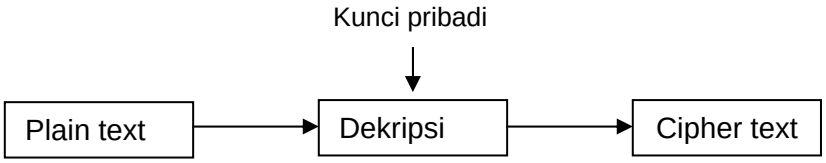
Enkripsi dengan cara ini menggunakan dua kunci yaitu satu kunci pribadi untuk enkripsi dan satu kunci publik untuk dekripsi. Algoritma dari enkripsi kunci publik adalah sebagai berikut :

a. Algoritma enkripsi pengiriman digambarkan dalam skema berikut:



Gambar 2.a. Algoritma Enkripsi Pengiriman

b. Adapun algoritma dekripsi penerimaan seperti skema di bawah ini:



Gambar 2.b. Algoritma Dekripsi Penerimaan

Dalam algorima kunci publik, kunci enkripsi dibuka sehingga tak seorangpun dapat menggunakannya, tetapi untuk dekripsi hanya satu orang yang punya kunci dan dapat menggunakannya. (Kristanto, 2003)

Percobaan dan Pembahasan

Pada artikel ini akan dilakukan percobaan penggunaan digit nilai desimal bilangan e dalam chipher hill yang diimplementasikan pada kode ASCII.

Cara enkripsi-dekripsi di dalam metode Hills menggunakan matriks bujur sangkar, misal matriks 3x3. Jika pada cipher hill yang biasa digunakan hanya diterapkan pada 26 karakter saja, sehingga untuk semua perhitungan matriks menggunakan modulo 26, maka pada cipher hill yang diimplementasikan pada kode ASCII yang mempunyai anggota sebanyak 256 karakter, maka semua perhitungan matriks menggunakan modulo 256. Contoh dipilih kunci = 4, maka elemen matriks diambil mulai dari digit ke 4 dari nilai desimal bilangan e, e=2.7182818284590452353602874713 52 …, yaitu:

$$M = \begin{bmatrix} 2 & 8 & 1 \\ 8 & 2 & 8 \\ 4 & 5 & 9 \end{bmatrix}$$

Misalnya akan dienkripsi sebuah pesan "**password=kuswari#1404**", dalam kode ASCII p ↔ 112, a ↔ 97, s ↔ 115, w ↔ 119, o ↔ 111, r ↔ 114, d ↔ 100, = ↔ 61, k ↔ 107, u ↔ 117, i ↔ 105, # ↔ 35, 1 ↔ 49, 4 ↔ 52, 0 ↔ 48, sehingga pesan **password=kuswari#1404,** menjadi 112 97 115 115 119 111 114 100 61 107 117 115 119 97 114 105 35 49 52 48 52. Dari nilai plaintext ini, digitnya dikelompokkan yang

mana anggotanya terdiri dari 3 elemen, maka diperoleh kelompoknya adalah (112 97 115), (115 119 111), (114 100 61), (107 117 115), (119 97 114), (105 35 49), (52 48 52), sehingga diperoleh *cipher*text untuk kelompok pertama (112 97 115) adalah

$$\begin{bmatrix}2 & 8 & 1\\ 8 & 2 & 8\\ 4 & 5 & 9\end{bmatrix}\begin{bmatrix}112\\ 97\\ 115\end{bmatrix}=\begin{bmatrix}1115\\ 2010\\ 1968\end{bmatrix}=\begin{bmatrix}91\\ 218\\ 176\end{bmatrix}$$ mod 256, dimana (91 218 176) adalah karakter **[┌s**

Untuk kelompok kedua dan seterusnya

$$\begin{bmatrix}2 & 8 & 1\\ 8 & 2 & 8\\ 4 & 5 & 9\end{bmatrix}\begin{bmatrix}115 & 114 & 107 & 119 & 105 & 52\\ 119 & 100 & 117 & 97 & 35 & 48\\ 111 & 61 & 115 & 114 & 49 & 52\end{bmatrix}=\begin{bmatrix}1293 & 1089 & 1265 & 1128 & 539 & 540\\ 2046 & 1600 & 2010 & 2058 & 1302 & 928\\ 2054 & 1505 & 2048 & 1987 & 1036 & 916\end{bmatrix}$$

$$=\begin{bmatrix}13 & 65 & 241 & 104 & 27 & 28\\ 254 & 64 & 218 & 10 & 22 & 160\\ 6 & 225 & 0 & 195 & 12 & 148\end{bmatrix}$$ modulo 256, dimana angka-angka matriks tersebut adalah karakter **CR■ACK, A@β , ± ┌ NUL, hLF ├, ESC SYN FF, FS á ö,** sehingga keseluruhan pesan dienkripsi dan dikirimkan menjadi pesan **[┌s CR■ACK A@β ± ┌ NUL hLF ├ ESC SYN FF FS á ö.**

Dari hasil enkripsi di atas, untuk mendekripsikan kembali ke bentuk asli maka kelompok 3 elemen dikalikan dengan M^{-1} modulo 256, yaitu sebagai berikut :

$$M^{-1}.\begin{bmatrix}91\\ 218\\ 176\end{bmatrix}=\begin{bmatrix}112\\ 97\\ 115\end{bmatrix}$$ dan seterusnya.

Implementasi cipher hills pada kode ASCII ini akan menghasilkan suatu deretan karakter yang tidak mudah untuk ditebak. Jika pada cipher hills yang diterapkan hanya untuk deretan 26 alfabet, salah satu contohnya adalah ‘spasi’ tidak dikodekan menjadi suatu bilangan atau karakter, sehingga cenderung lebih mudah untuk ditebak, tetapi pada kode ASCII ini semua simbol, spasi, operator dan sebagainya dapat dikodekan menjadi suatu bilangan, maka kemungkinan untuk menebak(mendekripsi) oleh orang yang tidak berhak akan menjadi lebih sulit dan semakin besar ukuran kunci yang digunakan pada cipher hill akan semakin menyulitkan orang yang tidak berhak mendekripsikan kembali pesan aslinya.

Kesimpulan

Implementasi cipher hills pada kode ASCII memberikan kemungkinan yang luas pada lebih banyak karakter yang tercakup, tidak hanya terbatas pada 26 alfabet, tetapi juga mencakup karakter-karakter seperti . ,", ',=,@,#,% dan sebagainya.

Keunikan digit desimal dari bilangan Euler (biasa disebut bilangan e) dapat digunakan sebagai acuan penerapan algoritma yang ada di kajian kriptografi, yang salah satunya adalah cipher hills. Hal ini dengan pertimbangan bahwa pembangkitan bilangan/kode acuan dapat diperoleh dari formulasi perhitungan digit desimal bilangan Euler yang sudah mapan dan diakui dunia.

Daftar Pustaka

Dence, Thomas P and Heath, Steven, *Using Pi in Cryptology*, Math Computing Education 39 no 1 winter 2005, Wilson Company, 2005

Kristanto, Andri, *Keamanan data pada Jaringan Komputer*, Gava Media, 2003

Levy, Silvio,*AffineTransformation,*1995, *http://www.geom.uiuc.edu/docs/reference/CRC-formulas/figshear*

Martyn Parker, *Gifted and Talented Enhancement Course:Codes and Ciphers* Mathematics Institute University of Warwick, 2005

O'Connor JJ and Robertson, E F, *History topic : The Number of e*, 2001, http://www-groups.dcs.st-and.ac.uk/history/printHT/e.html

Sami Dahlman, *Key management schemes in multicast environments* University of Tampere Department of Computer Science Pro gradu Thesis, 2001

Savard, John J.G, *The Hill Cipher*,1999. http://home.ecn.ab.ca/%7Ejsavard/crypto/ro020103.htm

Wibowo, Arrianto Mukti, *Studi Perbandingan Sistem-sistem Perdagangan di Internet dan Desain Protokol Cek Bilyet Digital* ,Universitas Indonesia,1997 http://www.geocities.com/amwibowo/resource.html

Hills Cipher, www.en.wikipedia.org/hills#cipher